Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

CMS Security Whitepaper:

Mainframe OS/390 and z/OS ACF2 Whitepaper

FINAL
Version 2.0
March 08, 2009

(This Page Intentionally Blank)

SUMMARY OF CHANGES IN *MAINFRAME OS/390 AND Z/OS ACF2* WHITEPAPER, VERSION 2.0

1) Converted baseline version dated March 7, 2007 to updated CMS style format.
2) Moved Section 1, Introduction, from before Table of Contents to after.
3) Updated Section 2, Background, to add BPSSM section reference concerning the use of STIGs.
4) Added titles to the following tables:
   a) Table 1 in Section 3.1.1.1,
   b) Table 2 in Section 3.1.3,
   c) Table 3 in Section 3.2.2,
   d) Table 4 in Section 3.2.6, and
   e) Table 5 and 6 in Section 3.3.1.
5) Removed former Appendix A CSRs and added pointer to new CMSRs.
6) Changed CSR glossary term in Appendix B to CMSR.
7) Updated the Appendix A CMSR reference.

SUMMARY OF CHANGES IN *MAINFRAME OS/390 AND Z/OS ACF2* WHITEPAPER, VERSION 1.0

1) Baseline Version 1.0.

(This Page Intentionally Blank)

TABLE OF CONTENTS

LIST OF TABLES

(This Page Intentionally Blank)

1 INTRODUCTION

This white paper was developed by PricewaterhouseCoopers LLP (PwC) for the Centers for Medicare and Medicaid Services (CMS). This document is one of a number of white papers issued by CMS management to assist with the proper understanding and implementation of key security controls around CMS' data and information systems environment.

The intended audience of this paper however, extends beyond CMS management and staff to include all CMS business partners. In this context, a CMS business partner is any private or public sector organization which provides services to this agency. These business partners include, but are not limited to; Medicare Carriers, Fiscal Intermediaries (FI), Common Working File (CWF) Host Sites, Durable Medical Equipment Regional Carriers (DMERCs), standard claims processing system maintainers, Regional Laboratory Carriers, claims processing data centers, Medicare Administrative Contractors (MAC), and Enterprise Data Centers (EDC).

This document is designed to provide guidance and information to CMS & CMS business partners in implementing and configuring a secure operating system (O/S) and computing environment through the use of the access control product ACF2. As computers and technology advanced they became capable of running several programs at once. This created a need to control resources and programs. The O/S addressed these issues by controlling the resources and functions that programs could use as well as keeping them from interfering with one another and the O/S itself. With the advent on online applications and transaction processing, it became possible for multiple end users to connect to a computer simultaneously, submitting and manipulating data from remote locations. Access control products (ACP) were developed to prevent users from affecting resources or processes outside of their responsibility. The O/S and ACP work in tandem to ensure the integrity of mainframe

O/S deployed by most CMS Contractor's mainframes use the International Business Machines (IBM) OS/390 or z/OS operating system package which includes the MVS O/S. The Defense Information Systems Agency (DISA), an agency of the Department of Defense (DOD), has developed an OS/390 & z/OS Security Technical Implementation Guide (STIG). The STIG, Version 5, Release 2, provides guidance on implementation of controls, configurations, and design of the OS/390,z/OS, and ACPs. References within this document to OS/390 also relate to z/OS; all references to OS/390 can also be applied to z/OS.

The purpose of this document is to relay pertinent information within the STIG to CMS and applicable CMS Contractors which process information on behalf of CMS utilizing OS/390 or z/OS. Information within this document does not cover all controls and guidance provided within the STIG nor should a contractor using just this information have comfort in the overall security and integrity of their O/S. Rather, this document should be used as an introduction to the STIG and information contained within used as a starting point in developing a secure and controlled environment. This document will focus on and the access control product known as ACF2, or Access Control Facility 2, produced by Computer Associates (CA).

2 BACKGROUND

Federal agencies, such as CMS and CMS contractors processing claims on their behalf, have become increasingly reliant on computerized information systems to process, maintain, and report essential information. This dependency on systems will continue to increase as technology advances and with this reliance also comes inherent vulnerabilities. To mitigate the risks associated with computerized information processing security and controls over the systems are paramount.

A key aspect of any computerized environment is the O/S. The O/S is used to control programs and resources, allowing multiple programs to run on the mainframe without interfering with one another or the O/S. Most federal agencies process many significant transactions through the use of a mainframe and use IBM OS/390 or z/OS. Additionally, agencies secure these environments with ACPs such as ACF2. Access control products (ACP) were developed to prevent users from affecting resources or processes outside of their responsibility. The O/S and the ACPs must be properly installed and configured to maintain the integrity of the site.

Secure configurations and controls of ACF2 are essential to the integrity of a processing environment and they are subject to review as part of financial statement audits. Federal audit requirements applicable to the audit of CMS' financial statements include assessing the general and application controls over the processing of Medicare information and concluding on whether the controls are operating effectively.

To assist in the appropriate configuration of ACF2, the DoD released the OS/390 & z/OS STIG, Version 5, Volume 2 on September 11, 2006. The STIG was developed by DISA for the DoD and provides guidance for the implementation and configuration of OS/390, ACF2, RACF, and TSS. This document was developed with regards to the STIG and key aspects of audit work programs in order to introduce concepts provided by the STIG. The STIGs provide very useful information on establishing a control framework for the mainframe operating system. This document will relay pertinent information from the STIG to readers, however, is not a substitute for the STIG, and will not alone provide a completely secure environment. Refer to section 3.10.2 in the BPSSM concerning the use of STIGS in the business partner environment.

3 ACF2 SECURITY IN THE OS/390 ENVIRONMENT

Multiple Virtual System (MVS) is an operating system which is part of the OS/390 and z/OS software packages. MVS controls programs and users and prevents them from interfering with one another and the O/S itself. When a user logs on to a terminal, when a batch job starts or a task, the System Authorization Facility (SAF), a component of MVS, makes a call to an Access Control Product (ACP). ACPs are security mechanisms that provide security controls for the OS/390 environment. ACPs, such as ACF2, RACF, and Top Secret, receive controls from SAF by means of the RACROUTE macro. The ACP will create a control block in memory called the ACEE (Access Control Environment Element). The ACEE will contain information in regards to the accesses allowed for a user, started task, batch job, etc. For example, when the user attempts to access a dataset or resource the ACP can get control to determine whether they should be permitted to access it. This is accomplished by comparing the information in the ACEE to either an ACF2 dataset rule or a resource rule.

The ACP uses records, dataset rules, and resource rules to secure access to data and resources. The ACP provides security by answering the following two questions:

1) Is the user who they say they are?

2) What resources, datasets, transactions, etc. do they have access to?

By authenticating a user and controlling their access the tool maintains the integrity of the O/S, hence, configuration and controls surrounding ACP are paramount to ensure this integrity.

3.1 ACF2 SYSTEM CONFIGURATION

3.1.1 SYSTEM CONFIGURATION STANDARDS

ACF2 offers many options with a variety of settings which can have a dramatic affect on the level of control that the ACP can provide. One such means of defining system options within ACF2 is by way of the Global System Options (GSO) records.

3.1.1.1 GSO SETTINGS

By establishing control in the GSO settings the entity can provide overall secure ACP parameters. However, settings can also be configured at the user level which can override global settings. Therefore, an entity cannot ensure the integrity of the O/S just be securing the GSO records. Weak settings at the global level can affect the overall security of the system. The types of risks vary based on the setting; some are further discussed within this document and the STIG. Further information is available in the CA-ACF2 Administrator Guide.

The DISA STIG recommends the following ACF2 Global Options and controls as specified below which will ensure the appropriate oversight and control of GSO. For additional information for each “policy bullet” including the short description identifier and the severity codes refer to the DISA STIG. Functions assigned to the Information Assurance Officer (IAO) should be performed by an individual with appropriate authority and knowledge.

The options specified below are STIG requirements and each site can choose to be more restrictive. The values listed below are deviations from product default settings. Values not listed are to be the default values for the product.

Table 1 Recommended Global Options Settings

Option	Description	Required Value
APPLDEF	Defines site-unique structured Infostorage records when standard structured Infostorage records will not suffice. Note: The APPLDEF record is optional. Use of this record will be justified in writing with supporting documentation.	Site Defined The IAO will ensure that the APPLDEF GSO record if used has supporting documentation indicating the reason it was used.
AUTHEXIT	Contains the vendor or site EXIT information that supports an extended authentication facility, such as operator identification (OID) card support.	GSO AUTHEXIT.001 record: LIDFIELD(AUTHSUP1) PROCPGM(AUTHXNCP) NOINFOSTG The IAO will ensure that the AUTHEXIT GSO value is used to define an extended user authentication EXIT is invoked at TSO logon, for Operator Identification (OID) card usage. DISA requires the use of NCPASS on all of its domains. DISA sites require the use of AUTHEXIT for other non DISA sites this value is optional.
AUTOERAS	Controls the automatic physical erasure of VSAM or non-VSAM data sets. CAUTION: Use of the Automatic Erase Feature can cause considerable system overhead affecting system performance.	Unclassified Systems: NONON-VSAM NOVSAM VOLS() Classified Systems: NON-VSAM VSAM VOLS(-) The IAO will ensure that the AUTOERASE GSO value indicates that you would like ACF2 to control the automatic physical erasure of VSAM or non-VSAM data sets. See above table for non-classified and classified values.
BACKUP	Controls automatic Security File backup.	Site defined. Note: a time must be specified unless the database is shared and backed up on another system. The IAO will ensure that the BACKUP GSO value specifies a time field and Time (00:00) is not specified unless the database is shared and backed up on another system.
BLPPGM	Specifies those programs authorized to use tape bypass label processing (BLP).	None will be specified. Note: BLP enforcement will be done based on LID record settings. The IAO will ensure the BLPPGM GSO value indicates that ACF2 does not control the programs authorized to use tape bypass label processing (BLP).

Option	Description	Required Value
CLASMAP	Translates an eight-character SAF resource class into a three-character ACF2 resource type code to enable resource rules to be written to perform validation. Also it translates the resource type codes for ACF2 calls or calls made to ACF2 from CA's International Standard Security Facility (CAISSF).	Vendor defaults as specified in the internal CLASMAP records unless as indicated otherwise below. The following resource class to resource type translations are the STIG recommended standard: APPL maps to APL CONSOLE maps to CON FACILITY maps to FAC OPERCMDS maps to OPR TSOAUTH maps to TSO The IAO will ensure the CLASMAP GSO value translates an eight character SAF resource class into a three-character ACF2 resource type code.

EXITS	Specifies the module names of site-written ACF2 EXIT routines.
	Note: The DSNPOST EXIT is optional and is not required to be specified in the GSO EXITS record.
		DSNPOST(module)
		SEVPRE(SEVPRE01)
		SEVPOST(SEVPST01)
		Note: No other exits are authorized at this time.
		Note: Local changes will be justified in writing with supporting documentation.
		The IAO will ensure the EXITS GSO value specifies the module names of site-written ACF2 EXIT routines. The above table indicates DISA defaults are optional for non-DISA sites.

LINKLST	Specifies one or more partitioned data sets considered part of the system link (SYS1.LINKLIB) during data set access validation.	Site defined. Only trusted system data sets will be listed. Application libraries will never be included. The IAO will ensure the LINKLIST GSO value if specified only contains trusted system datasets.
MAINT	Specifies the logonid, program, and library combinations used for system maintenance functions. Note: For logonids that match environments described in records, no SMF logging records will be created.	Site defined. Note: Entries will be restricted to production storage management user accounts and programs. The IAO will ensure the MAINT GSO value if specified will be restricted to production storage management user accounts and programs.

Option	Description	Required Value
NJE	Specifies ACF2 validation options that apply to jobs submitted through a network job entry subsystem (JES2, JES3, RSCS).	DFTLID() INHERIT NODEMASK(-) ENCRYPT VALIN(YES) NOVALOUT Note: For NJE nodes that are incompatible with the XDES algorithm, discrete NJE records will be created with NOENCRYPT. Note: Local changes will be justified in writing with supporting documentation. The IAO will ensure that the NJE GSO value indicates validation options that apply to jobs submitted through a network job entry subsystem (JES2, JES3, RSCS). See above table for values specified.
OPTS	Defines the global options available to the system.	BLPLOG NOCACHE NOCMDREC CONSOLE(NOROLL) CPUTIME(LOCAL) DATE(MDY) NODDB DFTLID() DFTSTC() INFOLIST(SECURITY, AUDIT) JOBCHK MAXVIO(10) MODE(ABORT) NOTIFY RPTSCOPE SHRDASD STAMPSMF STC TAPEDSN NOUADS NOVTAMOPEN The IAO will ensure that the OPTS GSO value is set to valid options specified in the above table. If not equal to specified settings, then it is a CAT II finding. If MODE does not indicate abort, then upgrade this finding to a CAT I finding.
PPGM	Defines protected programs that can only be executed by privileged users.	PGM-MASK(pgm-mask1, ...,pgmmask255) Refer to the table in Section 3.1.5.3, (Volume 1) Sensitive Utility Controls, for the minimal list of programs to be controlled. The IAO will ensure that the PPGM GSO value indicates protected programs that are only executed by privileged users.

Option	Description	Required Value
PSWD	Defines various logonid password options and controls. Note: If NOTE 12 is installed and its function is to increase the password history to 10 entries, set the GSO PSWD option to NOPSWDHST.	MAXTRY(3) MINPSWD(8) PASSLMT(5) PSWDALT PSWDFRC PSWDHST PSWDJES PSWDLID PSWDNCH PSWDNUM PSWDREQ PSWDRSV NOPSWDXTR WRNDAYS(10) The IAO will ensure that the PSWD GSO values are set to the values specified above.
RESRULE	Specifies data set access rules that are to be made resident at ACF2 initialization time.	None. Note: Local changes will be justified in writing with supporting documentation. The IAO will ensure that the RESRULE GSO value is set to NONE any other setting requires documentation justifying the change.
RESVOLS	Defines the DASD and mass storage volumes for which ACF2 is to provide data set-level protection.	VOLMASK(-) Note: Local changes will be justified in writing with supporting documentation. The IAO will ensure that the RESVOL GSO value is set to Volmask(-). Any other setting requires documentation justifying the change.
RULEOPTS	Specifies the options that determine how resource and access rules are used and maintained.	CENTRAL CHANGE DECOMP(SECURITY,AUDIT) NO$NOSORT RULELONG|NORULELONG NOVOLRULE The IAO will ensure that the RULEOPTS GSO values are set to the values specified above.
SAFDEF	Defines System Authorization Facility (SAF) calls that each site may want to process differently than the default ACF2 process.	Vendor defaults as specified in the internal SAFDEF records. Note: All vendor-modified and site-defined SAFDEF records will be justified in writing with supporting documentation.
SECVOLS	Defines those DASD, mass storage, and tape volumes for which ACF2 is to provide volume-level protection.	VOLMASK() Note: Local changes will be justified in writing with supporting documentation. The IAO will ensure that the SECVOLS GSO value is set to VOLMASK(). Any local changes are justified and documented with the IAO.

Option	Description	Required Value

SYNCOPTS	Defines the cache synchronization processing for a CPU running in a shared ACF2 database environment.	FILENAME(ACF2.SYNCFILE)
		POLLINTV(10)
		USECOUNT(10)
		NOACTIVATE
		The IAO will ensure that the SYNCOPTS GSO values are set to the values specified above.

TSO	Specifies global usage and system parameters that define and control the TSO logon process and other system parameters.	ACCOUNT(1)
		BYPASS(#)
		CHAR(BS)
		CMDLIST()
		NOFSRETAIN
		LINE(ATTN)
		LOGONCK
		PERFORM(0)
		PROC(IKJACCNT)
		NOQLOGON
		REGION(site defined)
		SUBCLSS()
		SUBHOLD()
		SUBMSG()
		TIME(0)
		TSOSOUT(A)
		UNIT(SYSDA)
		WAITIME(60) or less
		The IAO will ensure that the TSO GSO values are set to the values specified above.

TSOCRT	Defines a clear string used to obliterate the logon to ASCII CRT devices.	STRING(A12FA11C1A270C0D) The IAO will ensure that the TSOCRT GSO values are set to the values specified above.
TSOKEYS	Defines site-supplied keywords permitted by ACF2 at TSO logon time.	KEYWORDS() The IAO will ensure that the TSOKEYS GSO value is set to KEYWORDS().

TSOTWX	Defines a cross-out mask to obliterate the logon password on TWX devices.	CR(15)
		IDLE(17)
		LENGTH(8)
		M1(X)
		M2(N)
		M3(Z)
		M4(M)
		STRING()
		The IAO will ensure that the TSOTWX GSO values are set to the values specified above.

Option	Description	Required Value

TSO2741	Defines a cross-out string used to obliterate the logon password on 2741 devices.	BS(16)
		LENGTH(8)
		M1(X)
		M2(N)
		M3(Z)
		M4(M)
		STRING()
		The IAO will ensure that the TSO2741 GSO values are set to the values specified above.

UNIXOPTS	Specifies global options pertinent to the UNIX System Services (OMVS) environment. Note: DFTGROUP and DFTUSER should only be used for non classified systems using FTP. Restrictions apply. Refer to Section 2.5.2.6.2. Paragraph 7, 'Unprivileged Users and Groups' of this STIG for further information.	CHOWNRES DFTGROUP(defaultgroup) DFTUSER(defaultuser).

Refer to the DISA O/S 390 & z/OS STIG, V5R2, Section 3.2.1; Table A-. REQUIRED GLOBAL OPTIONS (GSO RECORDS).

3.1.1 ABORT MODE

The OPTS setting will display the mode that the main ACF2 system is in. This applies to all processing with the exception of IMS and CICS regions which contain their own MODE values or any portion of ACF2 processing affected by EXITS. ABORT is the only acceptable DISA setting. While running in the ABORT mode any access attempt not specified by the system will not be allowed and will be logged. Other settings are not allowable including; for example, the WARN setting which will allow unauthorized access with a warning message. Access that is not specified by the system will be allowed and logged. Likewise, LOG mode will allow unspecified access without a warning message. Access that is not specified by the system will be allowed and logged. It is obviously pertinent for organizations to ensure that they are operating ACF2 in ABORT mode, otherwise data set and resource rules and all ACP security will be overridden.

3.1.1 PASSWORD GUIDELINES

Passwords are used to validate a user to their logonid. Users should create their own passwords, which encourages them to not write them down. However, guidelines must be enforced over the composition of passwords to ensure that user created passwords impose security and cannot be easily guessed.

Weak password setting could allow unauthorized access to system resources or data by a user. By increases the strength of passwords the probability that passwords can be ‘cracked’ decreases significantly.

The DISA STIG recommends following the password guidelines specified below which will ensure the appropriate oversight and control of passwords; please note that responsibilities delegated to the IAO should be performed by an individual with appropriate knowledge and authority within the organization.

1) After three consecutive password failures, the userid is to be suspended until reset by the IAO or authorized personnel.

2) Passwords are to be eight (8) characters in length.

3) Passwords are to be a mix of alphabetic, numeric, and special characters, including at least one of each. Special characters include the national characters (i.e., @, #, and $) and other non-alphabetic and non-numeric characters typically found on a keyboard. However at this time the three ACPs only support the national characters. The following set represents the complete list of characters currently supported by the three ACPs:

    ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789@#$

    Note: Lower case alphabetic characters are not supported by the three ACPs.

4) Each character of the password is to be unique, prohibiting the use of repeating characters.

5) Passwords are to contain no consecutive characters (e.g., 12, AB).

6) Passwords are not to include the user’s name, telephone number, userid, or any standard dictionary word.

7) Users are to be required to change their password every 90 days at a minimum. Users are permitted to manage and change their own passwords.

8) Passwords are not to be changed more than once every 24 hours without the intervention of the IAO or authorized personnel.

9) Users are not to be permitted to reuse a password assigned within the last ten password changes.

10) The password files are to be stored in encrypted form.

11) Password requirements are to be enforced by standard security product controls where possible.

12) Exits are only to be used where the requirements cannot be enforced by standard security product controls. (Refer to the DISA STIG Section 3.1.3.2, Password EXIT Processing (volume 1), for further information.)

Note: Adherence is required when the software has the capability to enforce. Otherwise the password policies not enforced by the software are to be documented in the site Security Features Users Guide.

Refer to the DISA O/S 390 & z/OS STIG, V5R2, Volume 1, Section 3.1.3.1 Password Guidelines.

The above password requirements should be enforced by ACF2 by use of the ACF2 logonid (LID) record settings, the GSO PSWD record, and (optionally) the password validation EXIT (Refer to the DISA O/S 390 & z/OS STIG, V5R2, Volume 1, Section 3.2.3.2, Password EXIT Processing).

Most of the passwords requirements can be enforced by ACF2, however as noted within the DISA STIG, the below list cannot.

Table 2 Password Requirements Not Enforced by ACF2

Password Requirements not enforced by ACF2
No words found in standard dictionaries will be used.
At least one alphabetic, numeric, and special character will be used.
Each character of the password will be unique.
Passwords will contain no consecutive characters (e.g., 12, AB).
Passwords cannot be reused within 10 password changes.
Will not contain the user's name, userid (LID), or telephone number.

Where password standards cannot be enforced by ACF2 the STIG recommends use of EXITS. If this method is used, the following GSO EXITS record field should be used to implement these controls:

- NEWPXIT(module)

Refer to the DISA O/S 390 & z/OS STIG, V5R2, Volume 1, Section 3.2.3.2, Password EXIT Processing.

3.1.2 TSO PARAMETERS

ACF2 intercepts some OS/390 components and essentially gains control to decide if the request should be processed in one of three ways; allow, allow but log to SMF, and deny and log to SMF. ACF2 will make this choice based on the total environment and rules that specify access under certain conditions. Total environment considers components such as the user who made the request, the data set name, the program making the request, etc. TSO is one such component; TSO allows users to establish a session where they can issue commands.

Access to TSO is control by the TSO attribute within the Logonid record. TSO user attributes are taken from ACF2 and are specified by the appropriate default logon procedure (TSOPROC) and the Installation Account Code (IAC) (TSOACCT).

TSOPROC indicates a user’s default TSO procedure name.

TSOACCT specifies the user’s default TSO logon account.

Access to IACs can be controlled through use of ACF2 resource rules of TYPE(TAC) and access to TSO logon procedures will be strictly controlled using ACF2 resource rules of TYPE(TPR).

TSO initially runs as an APF-authorized program, which is turned off prior to invoking external commands and programs. However, TSO provides a way to allow APF-authorized programs to be executed in a TSO user’s address space. A program stored as a member of an APF library (an

APF-authorized program) can do virtually anything that it wants because it is essentially an extension of the O/S. It can put itself into supervisor state or obtain a system key, it can modify system controls, it can execute privileged instructions (while in supervisor state) and it can turn off logging to cover its tracks.

The process is controlled by the presence of the program name in one of two MVS load modules; SYS1.LINKLIB(IKJEFTE2) (for callable programs) and SYS1.LINKLIB(IKJEFTE8) (for TSO commands). The programs which are authorized are found in SYS1.PARMLIB(IKJTSOxx) and in load modules IKJTABLS and IKJEFTAP, which are located in SYS1.LPALIB.

Refer to the DISA O/S 390 & z/OS STIG, V5R2, Volume 1, Section 2.1.2.2 TSO APF Authorization.

The DISA STIG stresses control over a TSO command processor called PARMLIB. This command gives a user the ability to display and dynamically change the active IKJTSOxx member of SYS1.PARMLIB. A user with the ability to add or alter programs within IKJTSOxx could give a program APF-authorization which could execute as an authorized program within their address space. This could possibly give the program supervisor state, e.g. excessive privileges. The user would have access to the ACF2 PARMLIB resource of the ACF2 TSOAUTH resource class. This essentially bypasses security and gives a user privileges reserved to the O/S.

The DISA STIG recommends the following in regards to TSO controls; please note that responsibilities delegated to the IAO should be performed by an individual with appropriate knowledge and authority within the organization.

1) Only systems programmers responsible for supporting TSO/E should be authorized to access the PARMLIB command.

2) The following steps provide examples of ACF2 commands necessary to control the PARMLIB command:

   a) Create a three character resource type to be associated with the TSOAUTH resource class. The STIG required ACF2 resource type TSO should be used. Use the following parameters when creating a CLASMAP record:

      RESOURCE(TSOAUTH) RSRCTYPE(TSO)

   b) Define the PARMLIB resource to ACF2 and protect user access to the PARMLIB command by using the following ACF2 statements:

      i) Permit a user access to the PARMLIB command to display specifications in the active IKJTSOxx member:

         $KEY(PARMLIB) TYPE(TSO)

         UID(xxxxxxxx) SERVICE(READ) ALLOW

      ii) Permit a user access to the PARMLIB command to display and dynamically change the active IKJTSOxx member:

         $KEY(PARMLIB) TYPE(TSO)

UID(xxxxxxxx) SERVICE(READ,UPDATE) ALLOW

TSO can also be assigned privileged commands by ACF2. The ACP provides a means for assigning access to TSO/E commands through TSO privileges given to logonids. The DISA STIG states that controls will be in place to ensure that ACCTPRIV, CONSOLE, MOUNT, and OPERATOR privileges are restricted.

The DISA STIG provides the following techniques related to the above recommendations which further expand on the controls and the responsibilities of individuals within the organization. For additional information for each "policy bullet" including the short description identifier and the severity codes refer to the DISA STIG.

- The IAO will ensure that special privilege MOUNT is assigned only on an as needed basis for LOGONIDS associated with STCs and LOGONIDS that need to execute TSO in batch.
- The IAO will strictly control and limit the TSO privileges given to logonids. The privileges will be restricted to authorized personnel and justification for the privilege is documented.

Refer to the DISA O/S 390 & z/OS STIG, V5R2, Volume 1, Section 7.2.1 ACF2.

3.2 USER MANAGEMENT

3.2.1 USER CONTROLS

ACF2 provides many venues for controlling user access. The security product must be used to answer the question, who is this user and what do they have access to. ACF2 is used to determine if a user is allowed access to a resource or data set so it must be able to associate a user with each resource or data set they wish to access. Within ACF2 all users are identified by a user id, referred to as logonid. ACF2 users, batch jobs, and started tasks will all have a logonid. Logonids contain records which store information on the user which allows ACF2 to make decisions regarding what resources the user can access and what data they can read or update. Because each logonid is associated with certain privileges it is imperative that individuals have unique ids.

Without unique logonids users will be assigned access which may not enforce the concept of least privileged. Appropriate controls over access cannot be enforced with shared ids. In addition, logging will not be affective because the organization will not be able to appropriately determine which user performed the invalid function or violation. Thus there is no accountability.

In addition, ACF2 has default logonids associated with the product itself. Default ids are used as implementation aids. Because these ids are assigned to jobs there is a lack of control over the actual submitting user. Therefore a user could take advantage of the privileges of a default id.

The DISA STIG recommends the following in regards to logonid controls; please note that responsibilities delegated to the IAO should be performed by an individual with appropriate knowledge and authority within the organization.

1) Every user will be fully identified within ACF2. The following fields must be completed for every logonid.

   NAME - User's name

   UID-String - All fields defined in the ACFFDR @UID macro

2) All fields that comprise the standard UID string will be filled out for each user as a logonid is added.

The DISA STIG provides the following techniques related to the above recommendations which further expand on the controls and the responsibilities of individuals within the organization. For additional information for each “policy bullet” including the short description identifier and the severity codes refer to the DISA STIG.

- The IAO will ensure that all LOGONID records have the required attributes.
- The IAO will ensure that every user is uniquely identified to the system and that logonids are not shared among multiple users.

3.2.1 INTERACTIVE USERS AND PARAMETERS

As discussed above a logonid is made up of records which contain fields. Many fields are reserved for use by ACF2 and contain specific values for settings defined within ACF2 for each user. Default values are specified for all users when they are added to the system. These default settings can give a user privileges which would allow them to bypass security controls in place within ACF2.

For example, the following field ALLCMDS/NOALLCMDS can be set at the logonid level. If this field is set to ALLCMDS the user would have the ability to bypass the ACF2 restricted commands lists. This could allow that user to issue sensitive commands that would otherwise be protected. To further demonstrate this example consider the following; the SET PROG=xx command dynamically changes the EXIT definitions based on the information in the specified PROGxx member. The SETPROG EXITS command provides the capability to selectively add and delete EXIT routines from EXIT definitions. This command should be appropriately secured and may be restricted to operators; however, if a user was given ALLCMDS they could affectively issue this command and add or update an authorized EXIT. The user could use their updated EXIT to obtain supervisor state and have access to all data on the system.

Since logonids can override the global settings the default values must be appropriately controlled when a user is created within ACF2. The DISA STIG recommends the following in regards to logonid default controls; please note that responsibilities delegated to the IAO should be performed by an individual with appropriate knowledge and authority within the organization.

Table 3 Recommended logonid Default Control Settings

Field	Description	Required Value
ALLCMDS/ NOALLCMDS	Ability to bypass ACF2 restricted command lists.	NOALLCMDS

Field	Description	Required Value
AUTHSUP1	User Authorization Flag 1.	ON for highly privileged users controlled by NC-PASS. Note: Refer to Section 6.3.1, NC-PASS for ACF2, for further information.
CONSOLE/ NOCONSOLE	Permits access to the TSO/E CONSOLE facility.	NOCONSOLE The CONSOLE bit will not be turned on unless command-level controls are implemented.
GROUP(name)	This field is required for assigning gids to MVS OpenEdition users. Note: For sites running UNIX Systems Services, see Section 2.5.3.2, Defining Users and Groups, for GROUP(name) requirements.	Will be defined for OpenEdition users.
IDLE(time)	Specifies the maximum time permitted (in minutes) between terminal transactions for this user. If exceeded, ACF2 needs the logonid and password to be revalidated before another transaction is accepted. Zero (0) indicates no limit is enforced. This field is available for IMS and CICS on-line processing.	IDLE(15)
INTERCOM/ NOINTERCOM	Indicates this user is willing to accept messages from other users through the TSO SEND command.	INTERCOM
LGN-ACCT/ NOLGN-ACCT	Indicates permission to specify an account number at logon time. If a user has the PMT-ACCT field, ACF2 prompts the user for an account number unless an account number is specified before the prompt. If a user does not specify an account number at logon and PMT-ACCT is not specified in the user's logonid record, ACF2 uses the user's default account number (TSOACCT is the logonid field) or the system default account number. Specifies the default in the ACCOUNT field of the GSO TSO record.	LGN-ACCT
MAIL/NOMAIL	Indicates a user can receive mail messages from TSO at logon time.	MAIL
MAXDAYS(days)	Specifies the maximum number of days permitted between password changes before the password expires. Zero (0) indicates no limit.	MAXDAYS (90)
MINDAYS(days)	Specifies the minimum number of days that must elapse before a user can change a password. Zero (0) indicates no limit.	MINDAYS (1)
MOUNT/ NOMOUNT	Permission to issue mounts for devices.	NOMOUNT
MSGID/NOMSGID	Indicates this user wants TSO messages to have message IDs prefixed.	MSGID

Field	Description	Required Value
NAME(username)	Specifies the 1- to 20-character name of the user. ACF2 displays this name on logging and security violation reports. ACF2 also uses this name as the NAME field of the job statement created for a TSO logon session, if the NOUADS field is specified in the GSO OPTS record.	Will be completed for all users.
NON-CNCL/ NONON-CNCL	ACF2 cannot cancel the user for security violations. Access is permitted but logged.	NONON-CNCL
NO-STORE/ NONO-STORE	Specifies that a user cannot store or delete rule sets. This applies even if the value of the PREFIX field of the logonid record matches the $KEY of the rule of the data set, if the user has the SECURITY privilege, or if the user has change authority through a %CHANGE or %RCHANGE control statement in the rule set.	NONO-STORE Note: The GSO RULEOPTS record must specify CENTRAL. Refer to the GSO Options in Table A-30, Standard Global Options (GSO Records) - ACF2.
NOTICES/ NONOTICES	Indicates a user can receive TSO notices at logon time.	NOTICES
OPERATOR/ NOOPERATOR	User has TSO operator privileges.	NOOPERATOR
PASSWORD	The logon password for the user.	Must be completed.
PHONE	Specifies the 1- to 12-character telephone number of a user.	Optional
PMT-ACCT/ NOPMT-ACCT	Indicates that ACF2 requires a user to specify an account at logon time and to specify the LGN-ACCT field also. ACF2 does not prompt for an account number if the FSRETAIN field is also specified. FSRETAIN obtains account values from the last session.	May be required for Fee-for-Service support.
PPGM/NOPPGM	User can execute protected programs specified in the GSO PPGM record.	NOPPGM
PREFIX	User access to the user’s own data sets without rule validation.	PREFIX()
PROMPT/ NOPROMPT	Indicates that ACF2 prompts a user for missing or incorrect parameters.	PROMPT
RSRCVLD/ NORSRCVLD	Indicates that an access rule must validate any resource accesses that the user makes. Applies even if the user has ownership of the resource, or has the SECURITY attribute.	RSRCVLD
RULEVLD/ NORULEVLD	Indicates that an access rule must validate any data set accesses that the user makes. Applies even if the user has ownership of the data set, or has the SECURITY attribute.	RULEVLD
TSOACCT	Specifies the user's default TSO logon account. Used for all billing.	May be required for Fee-for-Service support.
TSOPROC	Specifies the user's default TSO logon procedure.	Will be completed for all TSO users.

Field	Description	Required Value
UID-String Fields	All fields defined in the @UID macro in the ACFFDR. UID-string fields currently are locally defined on each system. Their composition and contents will be fully documented by the IAO.	Will be completed. Note: Only those fields necessary to restrict the user to those accesses and functions required to perform assigned tasks are required.
VLD-ACCT/ NOVLD-ACCT	Indicates that ACF2 validates the TSO account number of a user. Creates a resource rule with a type code TAC and a $KEY of the account number so that ACF2 will perform this validation.	VLD-ACCT May be required for Fee-for-Service support.
VLD-PROC/ NOVLD-PROC	Indicates that ACF2 validates the TSO logon procedure of a user. Creates a resource rule with a type code TPR and a $KEY of the logon procedure so that ACF2 will perform this validation.	VLD-PROC Will be completed for all TSO users.

The DISA STIG provides the following technique related to the above recommendations which further expand on the controls and the responsibilities of individuals within the organization. For additional information for each “policy bullet” including the short description identifier and the severity codes refer to the DISA STIG.

- The IAO will ensure that all LOGONID records for interactive users have the required attributes. See above table for the values for each parameter.

Refer to the DISA O/S 390 & z/OS STIG, V5R2, Volume 1, Section 3.2.2.1 Interactive Users.

3.2.1 STC (STARTED TASK CONTROL) USERS

Started tasks are procedures started from the operating system console with the MVS START command. Like batch jobs, it is possible to assign an ACF2 logonid to started tasks to control the activities performed by a resources available to the started task. By default started tasks do not run under a specific userid, allowing the task to operate without being identified to ACF2. Without controls over this process, started tasks have the authority to access any information in the O/S.

Every started task should be uniquely identified to the ACP by the IAO. This will ensure that the resources available to the task are limited to only those resources deemed necessary. Additionally, it uniquely identifies the actions of the task in log data which can be used to trace system problems. Software Support personnel should notify the IAO so that a unique userid can be assigned to any new started task added to the system. No default userids are to be assigned to started tasks otherwise not identified.

Started tasks are stored as members in program libraries. It is possible that both started tasks and non-started tasks exist in the concatenated libraries. These typically are procedures intended for general use as batch processes or for use by TSO users. To prevent their improper execution, these members should not be defined to ACF2 as started tasks.

The DISA STIG recommends the following in regards to STC; please note that responsibilities delegated to the IAO should be performed by an individual with appropriate knowledge and authority within the organization.

1) The logonid for a Started Task Control (STC) will be granted the minimum privileges necessary for the STC to function. In addition to the default LID field settings, all STC logonids will have the following field setting:

   STC

2) If the STC is a Multi User Single Address Space System (MUSASS), the STC logonid will also have the following attributes:

   MUSASS

   NO SMC

3) If the Multi User Single Address Space System (MUSASS) has the requirement to submit jobs on behalf of its users, the STC logonid will also have the following attribute:

   JOBFROM

4) If the Multi User Single Address Space System (MUSASS) has the requirement to update information in the ACF2 database on behalf of its users, the STC logonid will also have the following attribute:

   MUSUPDT

5) The use of default IDs prevents the identification of tasks with individual users as mandated by policy, and prevents adequate accountability. Default IDs for STCs will not be used.

6) Certain started tasks performing critical operating system related functions may be considered trusted for the purposes of data set and resource access requests. For these STCs all access requests will be honored. These STCs will be given the following attribute to facilitate access while logging any accesses they would not ordinarily be granted by the access rule sets:

   NON CNCL

The DISA STIG provides the following techniques related to the above recommendations which further expand on the controls and the responsibilities of individuals within the organization. For additional information for each “policy bullet” including the short description identifier and the severity codes refer to the DISA STIG.

- The IAO will ensure that all logonid records assigned to started tasks have the STC attribute specified.

- The IAO will ensure that if the STC is a Multi User Single Address Space System (MUSASS), the STC logonid has the MUSASS and NO SMC attributes.

- The IAO will ensure that if the Multi User Single Address Space System (MUSASS) has the requirement to submit jobs on behalf of its users, the STC logonid has the JOBFROM attribute specified.

- The IAO will ensure that if the Multi User Single Address Space System (MUSASS) has the requirement to update information in the ACF2 database on behalf of its users, the STC logonid has the MUSUPDT attribute specified.

- The IAO will ensure that only STC in the trusted STC list can have the NON-CNCL attribute and any other STCs having this attribute are approved by the site DAA (designated approving authority, such as a system owner).

Refer to the DISA O/S 390 & z/OS STIG, V5R2, Volume 1, Section 3.2.2.3 Started Task Control (STC) User.

3.2.2 EMERGENCY ACCESS USERS

Any processing environment will have situations that arise that are required to be immediately resolved so that data processing can occur. During these emergencies personnel may need elevated levels of access with additional privileges. To handle these situations emergency ids, also referred to as super ids or firecall ids, may need to be enacted.

Since these logonids generally have access which will bypass system security, such as NON-CNCL, they must be secured so that individuals do not have general access to them, if used they must be logged and reviewed, and access should be automatically revoked after a period of time.

The DISA STIG recommends the following in regards to emergency access controls; please note that responsibilities delegated to the IAO should be performed by an individual with appropriate knowledge and authority within the organization.

1) One class of userids are to exist to perform all operating system functions except ACP administration. These super IDs may be released according to STIG recommended policy to effect repairs of the operating system in emergencies.

2) A second class of super IDs is to be maintained to allow the functions associated only with ACP administration. These IDs are to only be released at the direction of the IAO.

3) Normally both super IDs are not to be released to the same individual concurrently, although approved exceptions to this rule can be made. This constraint effects a check and balance process for recovery situations requiring both forms of authorization.

4) The super IDs are to be implemented with logging to provide an audit trail of their activities.

5) Both classes of super IDs are to be maintained in both the ACP and SYS1.UADS to ensure they are available in the event that the ACP is not functional.

6) Each super ID is to have distinct, different passwords in SYS1.UADS [user attribute data set] and in the ACP, and the site is to establish procedures to ensure that the passwords differ. The password for any ID in SYS1.UADS is never to match the password for the same ID in the ACP.

7) Documented procedures are to be established to provide a mechanism for the use of the IDs. Their release for use is to be logged, and the log is to be maintained by the IAO. When a super ID is released for use, its password is to be reset by the IAO within 12 hours after it is no longer needed for problem resolution.

Refer to the DISA O/S 390 & z/OS STIG, V5R2, Volume 1, Section 3.1.2.6 Emergency Userids.

3.2.3 EMERGENCY PRIVILEGED ACCESS IN ACF2

As discussed above the STIG recommends use of two emergency ids, one located in SYS1.UADS in the case that the ACP is not functional and one in the ACP.

The DISA STIG recommends the in regards to emergency access; please note that responsibilities delegated to the IAO should be performed by an individual with appropriate knowledge and authority within the organization.

1) For emergency IDs with the ability to access and update all system data sets, but which do not have security administration privileges:

    NOFSRETAIN

    JCL

    JOB

    MONITOR

    NON CNCL (Will force logging of all activity.)

    TSO

    TSOPROC(xxxxxxxx)

    TSOACCT(none)

2) For emergency IDs with security administration privileges, but which cannot access and update system data sets:

    ACCOUNT

    NOFSRETAIN

    JCL

    JOB

    MONITOR

    NONON CNCL

    RULEVLD

    SECURITY

    TSO

    TSOPROC(xxxxxxxx)

    TSOACCT(none)

The DISA STIG provides the following techniques related to the above recommendations which further expand on the controls and the responsibilities of individuals within the organization. For additional information for each “policy bullet” including the short description identifier and the severity codes refer to the DISA STIG.

- The IAO will ensure that Emergency Logonids use the above fields to enforce restrictions as noted above and itemized in the DISA STIG [volume 1], Section 3.1.2.6, Emergency Userids.

Refer to the DISA O/S 390 & z/OS STIG, V5R2, Volume 1, Section 3.2.2.6.1 Privileged Access Emergency Userids.

3.2.4 PRIVILEGED ACCESS USERS

Every ACP provides attributes (types of privileges) that can allow a user to modify the security environments, perform auditing tasks, and circumvent security. These attributes within ACF2 are defined within their logonid record.

Within ACF2 these attributes must be controlled because of the privileges that they allow; privileges that could override security controls in place. Those of most importance include SECURITY, ACCOUNT, AUDIT, LEADER, CONSULT, TAPE-BLP, and TAPE-LBL.

In addition the most powerful attribute that can be assigned in NON-CNCL. This attribute should be strictly controlled as it allows a user to bypass all security controls in place and have free reign to access and update data.

The attributes are described below in further detail:

Table 4 User Privilege Attributes

Attribute	Users & Privileges
SECURITY	An unrestricted user with SECURITY, also known as a system administrator, and no scope limitations can perform the following: Create, change, list or delete any rule record or ACF2 infostorage record (an infostorage record defines system options such as to specify record-level protection expressions, defines extended user authentication records that store information about logonids. They have individual records that allow one to define and change fields individually, e.g. change values such as UADS to NOUADS). Access any resource even if a permitting rule is non-existent, he or she has the authority to create or change the rule. NOTE – ACF2 will log access by a user with SECURITY that is not specifically authorized by ACF2 rules. Execute any program on the restricted programs list (PPGM). Change and display certain fields in logonid records that no other users can change. NOTE – Privileges related to changing selected logonid record fields are modifiable by the organization. An individual with SECURITY and ACCOUNT can establish or delete logonid records; however, SECURITY alone will not allow this. Any security administrator (restricted or unrestricted) can use various TSO ACF subcommands not available to the normal user (such as SHOW STATE, SHOW ACTIVE, and SHOW TSO). Note: Organizations can restrict the rights of a user with the SECURITY attribute by use of a scope record. The record is SCPLIST field of the user logonid record. Restricted users have full SECURITY privileges but can only apply them to rules, records, and logonid records that fall within the outlined scope.

Attribute	Users & Privileges
ACCOUNT	Users with the ACCOUNT attribute, also known as account managers, can perform the following: Establish, maintain, view, and delete logonid records. Display the records and the parameters of the ACF2 system. Users with no scope limitations can execute the SYNCH command to synchronize the ACF2 login database with the TSO BROCAST data set. Use various SHOW subcommands which will display a large number of individual logonid fields. These fields can be defined by the site based on scope records assigned to them. As noted above a user with both SECURITY and ACCOUNT can establish or delete logonid records; this is a powerful combination. In addition, a user with only one attribute cannot modify the logonid record of a user with both attributes.
AUDIT	Users with the AUDIT attribute, also known as auditors, can perform the following: Display all records in any ACF2 database and use the SHOW subcommands. Please note that AUDIT does not provide the ability to update or delete any of these records or access any resources except those specifically authorized to him or her based on access rights and resource rules. Additional Notes: By the use of scope records this user can be restricted to only certain rules, logonid records and infostorage records. The READALL privilege can be set to grant an auditor or any other user for that matter the right to read and execute all data sets at the site regardless of access rules. Note this is similar to NON-CNCL with the difference being READALL only grants read and execute access.
LEADER	Users with the LEADER attribute can perform the following: Display most logonid records and has additional abilities for updating selected fields of the logonid records defined by the organization. Additional Notes: The attribute does not grant any special abilities in regards to the rule or infostorage database. Generally the attribute is not to powerful unless combined with ACCOUNT. However, scope records should be used to limit access.
CONSULT	Users with the CONSULT attribute, also known as consultants who assist users, can perform the following: Display most fields of logonid records and update only some non-security type fields related to TSO. Organizations can determine the fields which these users can display and update through scope records.
TAPE-BLP	Users with the TAPE-BLP attribute can use full bypass label processing (BLP) when accessing tape data sets. Please note that BLP allows a user to specify any data set or volume name within the JCL (job control language) without comparing the information with the tape label. If the user specifies BLP, ACF2 will allow the user to run the job specified. Therefore ACF2 will allow the user to override security controls in place for that certain tape label. This is a very powerful attribute that allows users to bypass security.
TAPE-LBL	Users with the TAPE-LBL attribute have limited access when using tapes. A user with this privilege requests a BLP request and ACF2 will check the actual volume serial number written on the tape label. If the actual volser (serial numbers of the volumes where the data sets reside) is available from the tape it will override the once specified in the JCL. The data set name used is the one from the JCL. The actual tape data set validation depends on the TAPEDSN field of the GSO OPTS record and whether the volser is specified in the GSO SECVOLS record.

Attribute	Users & Privileges
NON-CNCL	Users with this very powerful privilege have full access to any data set or resource regardless of violations that may occur during the attempt to access data or resources. Violations will be logged by ACF2 however, the logonid can access a data set or resource without logging as long as access is defined by a data access or resource rule or is permitted by the logonid PREFIX field. However, with access to all data sets a user could potentially alter logs. In addition an organization cannot create scope records to limit the access of a logonid with the NON-CNCL privilege. This attribute overrides all security that is in place and is extremely powerful.

The DISA STIG recommends the following in regards to privileged access; please note that responsibilities delegated to the IAO should be performed by an individual with appropriate knowledge and authority within the organization.

1) Only the IAO is to be given any privileges that can modify the security environment, such as changing system wide options.

   Note that while the DISA STIG recommends that only the IAO should have privileges to modify the security environment it is understandable that other authorized users may require such functionality. However, all access should be granted based on least privilege, authorized, logged, and monitored.

2) Users allowed to perform security administration for application related data are to be limited by the ACP to only change properties for which the user is responsible.

3) Privileges to view the contents of the security database may be granted to individuals by the IAO, provided a valid need exists. In many data centers, this access may be required for interactive system programmers to work with the user community to resolve problems.

4) Access to privileges to perform tape bypass label processing (BLP) is to be tightly controlled and only given to those authorized data center individuals (e.g., the tape librarian, Operations staff, or user) who require such access. Tape label bypass privileges allow a user to access data on a tape, using BLP processing, and, as such, to bypass any security related controls. Therefore, authorization to perform BLP processing by the user community is to be tightly controlled. This is because a severe exposure exists in that any data on any tape can be accessed.

5) In addition to the special privileges specifically noted above, many other special privileges pose the danger of compromising the operational environment when misused or improperly applied. Each ACP provides the ability to control these privileges and to restrict them only to those personnel with valid requirements for their use. These special privileges include, but are not limited to, the ability to do the following tasks:

   - Mount tape volumes to a TSO session.
   - Access system console information.
   - Issue console commands.
   - Execute restricted programs.

- Access data and resources despite rule restrictions.

6) Restrict access to special privileges only to those individuals with an authorized need. Grant access to the minimum level necessary for the performance of job requirements.

Refer to the DISA O/S 390 & z/OS STIG, V5R2, Volume 1, Section 3.1.4.1 Access Control Product Modification Privileges, 3.1.4.2 Audit Privileges, 3.1.4.3 Tape Label Bypass Privileges, 3.1.4.4 Other Sensitive Privileges.

The DISA STIG recommends the following in regards to privileged access attributes within ACF2; please note that responsibilities delegated to the IAO should be performed by an individual with appropriate knowledge and authority within the organization.

1) The special privileges discussed in this section are all of an extremely sensitive nature and will be rigidly controlled. The number of authorized users granted these privileges will be kept to an absolute minimum. Their use will be fully documented. The IAO will maintain the written request, justification, and authorization.

2) The following user privileges allow update of the ACF2 databases for administering users, data set access rules, and Infostorage records. When granted to a logonid, restrict the scope of the following privileges using an associated SCPLIST (scope list) record:

   ACCOUNT

   LEADER

   SECURITY

3) If a logonid is granted the SECURITY privilege, it is mandatory that RULEVLD and RSRCVLD attributes will also be specified for the logonid.

4) The following privileges cannot be scoped, and will be restricted exclusively to a site IAO:

   ACCTPRIV

   REFRESH

5) The following user privileges allow viewing of the ACF2 databases for the purpose of inspecting users, data set access rules, and Infostorage records. When granted to a logonid, restrict the scope of the following privileges using an associated SCPLIST (scope list) record:

   AUDIT

   CONSULT

6) The READALL privilege is available for actual auditing of system data. It gives the capability of looking at every data set on the system despite the data set rules. Its use is strongly discouraged. Always grant access through the use of standard data set access rules. Under no circumstances will the privilege be used as a convenience to the person maintaining the rule sets. Only use this privilege when absolutely necessary, and only give it to auditors. Remove the privilege once the audit is complete. Fully document the granting and revoking of the access.

7) Tape label bypass (BLP) privileges will be restricted at the user level. Specify one of the following two logonid privileges to grant a user access to BLP processing:

   User LID Record:

   TAPE LBL

   TAPE BLP

8) It is possible to grant selected programs to bypass tape label processing regardless of the BLP related privilege of the logonid executing the program.

9) This capability will not be used due to the requirement that accounting of BLP processing be done at the user level. Do not utilize the GSO BLPPGM record.

The DISA STIG provides the following techniques related to the above recommendations which further expand on the controls and the responsibilities of individuals within the organization. For additional information for each "policy bullet" including the short description identifier and the severity codes refer to the DISA STIG.

- The IAO will ensure logonids with the ACCOUNT, LEADER, SECURITY attributes are restricted by a SCPLIST attribute that restricts authority based on job function and area of responsibility.

- The IAO will ensure Logonids with the SECURITY attribute have the RULEVLD and RSRCVLD attributes specified.

- The IAO will ensure Logonids with the REFRESH attribute are only reserved for use by the IAO/IAM.

- The IAO will ensure Logonids with the ACCTPRIV attribute are only reserved for use by the IAO/IAM.

- The IAO will ensure that logonids with the AUDIT or CONSULT attributes are restricted by a SCPLIST attribute that restricts authority based on job function and area of responsibility.

- The IAO will ensure that procedures are in place to control Logonids with the READALL attribute.

- The IAO will ensure Logonids with the TAPE-LBL or TAPE-BLP are kept to a minimum and are controlled and documented.

- The IAO will ensure that special privilege MOUNT is assigned only on an as needed basis for LOGONIDS associated with STCs and LOGONIDS that need to execute TSO in batch.

- The IAO will ensure that access to the special privilege OPERATOR is kept to a minimum and is controlled and documented.

- The IAO will strictly control and limit access to TSOAUTH privileges. Authorization is restricted to authorized personnel; and justification for access is documented.

- The IAO will ensure that access to the special privilege ALLCMDS is kept to a minimum and is controlled and documented.

- The IAO will ensure that access to the special privilege PPGM is kept to a minimum and is controlled and documented.
- The IAO will ensure that only STC in the trusted STC list can have the NON-CNCL attribute and other STCs having this attribute are approved by the site DAA such as they system owner.

Refer to the DISA O/S 390 & z/OS STIG, V5R2, Volume 1, Section 3.2.4 Special Privilege Access, 3.2.4.1 Access Control Product Modification Privileges, 3.2.4.2 Audit Privileges, 3.2.4.3 Tape Label Bypass Privileges, 3.2.4.4 Other Sensitive Privileges.

3.3 RESOURCE CONTROLS

ACF2, RACF, and TSS provide capabilities to control access to system resources. System resources include data sets, volumes, spool volumes, sensitive utilities, and other programs, for example. Control of access to these resources is critical to ensure the integrity of the operating environment. For example, inappropriate access to PARMLIB could allow an individual to place an unauthorized program into an APF authorized library thus allowing the program to gain supervisor state. By gaining this access the program would have privileges usually reserved for the O/S. The user could have full access to data sets and make alterations to payroll data.

The DISA STIG provides information relating to data set controls, volume controls, sensitive utility controls, dynamic list controls, console controls, and system command controls. The following will focus on ACP controls for sensitive utilities, dynamic control lists, console access, system commands and transaction control.

3.3.1 CONTROLLING SENSITIVE UTILITIES

Sensitive utilities such as OMEGAMON, CICS, DASD, ICKDSF, etc. are required in most data centers to support various operations and processing. These products must be appropriately controlled as they are allowed to operate with privileges normally reserved for the OS. If a user could abuse the privileges of these programs they could potentially gain access to operate in supervisor state or with a protect key of 0-7. This could result in system failure, data manipulation, and bypassing of security in place. Therefore access to these programs should be very restricted. ACPs can be used to protect the utilities from unauthorized access at the program level.

The DISA STIG provides the following table of sensitive utility types and the type of user that should be granted access.

Table 5 Sensitive Utility Type/User

Sensitive Utility Controls	
UTILITY TYPE	LEGITIMATE USERS
Tape Management	Tape Librarian
DASD Management	DASD Management staff

Sensitive Utility Controls	
Job Scheduling	Production Control
Storage Alteration	Systems Programming
System Modification	Systems Programming

The DISA STIG provides the following table which displays a sample list of the minimal entries to be controlled:

Table 6 Sensitive Utility Controls

Sensitive Utility Controls		
PROGRAM	PRODUCT	FUNCTION
***GTF**	OS/390	System Activity Tracing
***IOCP	OS/390	System Configuration
*MASPZAP	OS/390	Data Management
AMAZAP	OS/390	Data Management
BLSROPTR	OS/390	Data Management
DEBE	OS/DEBE	Data Management
DITTO	OS/DITTO	Data Management
FDRZAPOP	FDR	Product Internal Modification
GIMSMP	SMP/E	Change Management Product
ICKDSF	OS/390	DASD Management
IDCSC01	OS/390	IDCAMS Set Cache Module
IEHATLAS	OS/390/DFP	Data Management
IEHD****	OS/390/DFP	DASD Management
IEHINITT	OS/390	Tape Management
IFASMFDP	OS/390	SMF Data Dump Utility
IGWSPZAP	OS/390	Data Management
IND$FILE	OS/390	PC to Mainframe File Transfer (Applicable only for classified systems)
*****SCP	OS/390	System Configuration
WHOIS	OS/390	Share MOD to identify user name from USERID. Restricted to data center personnel only.

The DISA STIG recommends the following in regards to controlling sensitive utilities by use of ACF2; please note that responsibilities delegated to the IAO should be performed by an individual with appropriate knowledge and authority within the organization.

1) Access to sensitive utilities will be strictly controlled. Access to the data sets in which the utilities reside will be controlled through the use of data set rules. Execution access will be controlled and monitored through the use of the MAINT, PPGM, and LOGPGM facilities.

2) Maintenance utilities will be controlled as described within Section 3.1.2.5, Special Storage Management Users. A GSO MAINT record will exist for each library containing maintenance utilities. Each record will identify the appropriate special user logonid and the programs that it is permitted to process. The associated special user logonid will contain the MAINT attribute to allow it to execute the identified utility programs. It is imperative to note that access rule validation or SMF logging will not be performed for these utility and logonid combinations.

3) Sensitive utilities, which are to be available to a limited number of users, will be identified in the Protected Program List (the GSO PPGM record). Authority to execute the identified programs is identified by the logonid record PPGM attribute. Standard access rule validation and SMF logging will be performed by ACF2. To restrict access for the utilities so that only certain utilities can be executed by certain individuals, the DSNPOST exit may be used. The exit will use the following process:

   - Programs that are to be restricted are coded in the GSO PPGM record. Users will not be given the PPGM privilege as a standard.

   - Based upon a PPGM violation, the exit code will validate an ACF2 resource rule type of PGM to further interrogate the use of the utility. Based upon the action in the PGM resource rule, the user will be allowed or disallowed the usage of the program.

4) The resource rules for program validation will look like the following:

   $KEY(pgm name) TYPE(PGM)

   UID(uid string) ALLOW

5) Standard data set access rules are required and will be written for the library or libraries containing the utility programs.

6) Audit access to protected programs considered sensitive in nature. These programs will include, at a minimum, those specified in Section 3.1.5.3, Sensitive Utility Controls (or refer above to Sensitive Utility Control table).

7) Sensitive utilities that are to be generally available, but whose use is to be audited, will be identified in the GSO LOGPGM record. The default values supplied by ACF2 will not be removed from the record. No special logonid record attribute is required to execute these programs. Standard access rule validation and SMF logging will be performed by ACF2. Standard data set access rules are required and will be written for the library or libraries containing the utility programs.

The DISA STIG provides the following technique related to the above recommendations which further expand on the controls and the responsibilities of individuals within the organization. For additional information for each “policy bullet” including the short description identifier and the severity codes refer to the DISA STIG.

- The IAO will ensure access to sensitive utilities is protected by ACF2 by using the resource rule TYPE(PGM). Only appropriate personal are to access and all access is logged.

Refer to the DISA O/S 390 & z/OS STIG, V5R2, Volume 1, Section 3.2.5.3 Sensitive Utility Controls.

3.3.1 DYNAMIC CONTROL LIST

As documented above MVS provides capabilities to perform dynamic changes within the O/S. Specifically, inherent to MVS, dynamic maintenance can be performed on EXITS and APF Libraries. The capability to perform dynamic EXIT maintenance is controlled by the CSVDYNEX macro, the SYS1.PARMLIB(PROGxx) member, the SET PROG=xx command, and the SETPROG EXITS command. The command SET PROG=xx dynamically changes the EXIT definitions based on the information in the specified PROGxx member. The SETPROG EXITS command provides the capability to selectively add and delete EXIT routines from EXIT definitions.

Without appropriate controls in place users could dynamically update libraries to be APF authorized, which could provide a means to obtain supervisor state. In addition, users could update EXITS and insert code that would allow them to obtain special privileges. Without appropriate control the organization cannot ensure the integrity of the O/S. These facilities, if made available to operators are to be controlled.

The DISA STIG recommends the following in regards to controlling dynamic control listings; please note that responsibilities delegated to the IAO should be performed by an individual with appropriate knowledge and authority within the organization.

1) Define the following resources in the FACILITY class with a default access of none:

   CSVAPF.**

   CSVAPF.MVS.SETPROG.FORMAT.DYNAMIC

   CSVAPF.MVS.SETPROG.FORMAT.STATIC

   CSVDYNEX.**

   CSVDYNL.**

   CSVDYNL.UPDATE.LNKLST

2) Limit authority to those resources to Systems personnel. Restrict this access to the absolutely minimum number of personnel, and log all accesses.

3) Limit authority to the SET PROG=, SETLOAD, and SETPROG commands to Systems personnel. Restrict this access to the absolutely minimum number of personnel, and log all accesses. For additional information refer to the DISA STIG section 3.1.5.6, OS/390 System Command Controls [volume 1].

Within ACF2 dynamic lists controls are provided by resources in the FACILITY resource class. The DISA STIG recommends the following in regards to controlling dynamic control listings by use of the FACILITY CLASS. Note that the FACILITY CLASS is used to validate resource rules. Resource validations are invoked for the security class of FACILITY.

1) Prevent access to these resources by default, and log all access. Create generic and specific resource rules as follows:

```
$KEY(CSVAPF) TYPE(FAC)
    - UID(-)
    MVS.SETPROG.FORMAT.DYNAMIC UID(-)
    MVS.SETPROG.FORMAT.STATIC UID(-)
$KEY(CSVDYNEX) TYPE(FAC)
    - UID(-)
$KEY(CSVDYNL) TYPE(FAC)
    - UID(-)
    UPDATE.LNKLST UID(-)
```

2) The required access to specific resources is to be discretely granted to specific systems users. Restrict this access to the absolutely minimum number of personnel, and log all access. Sample rules are as follows:

```
$KEY(CSVAPF) TYPE(FAC)
    SYS1.NEWLIB UID(-)
    SYS1.NEWLIB UID(sysprog) SERVICE(READ) LOG
```

The DISA STIG provides the following technique related to the above recommendations which further expand on the controls and the responsibilities of individuals within the organization. For additional information for each “policy bullet” including the short description identifier and the severity codes refer to the DISA STIG.

- The IAO will ensure that Issuing of Dynamic List Commands are defined to the FACITITY resource class and protected. Only system programmers and a limited number of authorized people are able to issue these commands. All access is logged.

Refer to the DISA O/S 390 & z/OS STIG, V5R2, Volume 1, Section 3.2.5.4 Dynamic List Controls.

3.3.1 CONTROLLING CONSOLE ACCESS

Consoles allow a user to directly enter operator commands without being validated by a unique user name or password. Any actions taken cannot be logged to a specific user but rather the console from which the commands were entered. Therefore, with consoles, there is limited accountability. Console commands are very powerful and can be used for a variety of functions, such as updating APF authorized libraries, system parameters within PARMLIB, or EXITS.

Therefore access to consoles must be stringently controlled as any user with physical access to a console can enter such commands.

Normally consoles are located within a physically secured area such as the computer room within a data center. However, just securing consoles within a restricted area may not be adequate because of remote console access. This access allows authorized personnel the ability to log into a console session and issue commands outside of the secured area. The ability to log the remote access is available, however, any actions completed after logging into the console cannot be traced back to the user. These commands will be attributed to the console being used at the time. The SYS1.PARMLIB(CONSOLxx) member is used to control consoles; a very limited number of operators should be provided this access.

The DISA STIG recommends the following in regards to controlling console access; please note that responsibilities delegated to the IAO should be performed by an individual with appropriate knowledge and authority within the organization.

1) Give every console an explicit console ID, and define that ID to the ACP as a user with only those access rights required for use of the console. Define every console, including extended MCS [multiple console support] consoles, with AUTH(INFO).

2) In SYS1.PARMLIB(CONSOLxx), specify the parameter LOGON(REQUIRED) on the DEFAULTS statement so that all operators are required to log on prior to entering OS/390 system commands. At the discretion of the IAO, LOGON(AUTO) may be used, provided the console userids are only authorized to use the CONTROL, DISPLAY, MONITOR, STOPMN, STOPTR, and TRACK commands, and their access is limited to read level.

3) The IAO will implement and document controls as described in the DISA STIG, Section 3.1.5, Resource Controls (volume 1).

Refer to the DISA O/S 390 & z/OS STIG, V5R2, Volume 1, Section 2.1.2.12 MCS Consoles.

Within ACF2 MCS (multiple console support) console controls are provided through resources in the CONSOLE, FACILITY, OPERCMDS, and TSOAUTH resource classes. These classes should already be active, and OPERCMDS should already use generic masking, but the sample commands shown below include the relevant ACF2 commands for the sake of completeness.

The DISA STIG recommends the following in regards to controlling console access within ACF2; please note that responsibilities delegated to the IAO should be performed by an individual with appropriate knowledge and authority within the organization.

1) Prevent access to these resources by default, and log all access. Create generic and specific resource rules as follows:

```
$KEY(consname) TYPE(CON)
    UID(-)
    UID(opermask) SERVICE(READ) LOG
$KEY(MVS) TYPE(OPR)
    UID(-)
```

```
$KEY(CONSOLE) TYPE(TSO)
     UID(-)
```

2) The user profile for each real MCS console is to be granted read access to the corresponding console resource:

```
$KEY(consname) TYPE(CON)
     UID(consname) ACCESS(READ) PERMIT
```

3) The user profiles for operators and systems programmers allowed to use each real MCS console should be granted read access to the corresponding console resource:

```
$KEY(consname) TYPE(CON)
     UID(opermask) ACCESS(READ) PERMIT
```

4) At the discretion of the IAO, users may be allowed to use the TSO CONSOLE command. This command is subject to the restrictions that are documented within the DISA STIG in Section 3.1.5.5, MCS Console Controls, Section 3.1.5.6, OS/390 System Command Controls, and Section 3.2.5.6, OS/390 System Command Controls (Volume 1). To grant the access, issue the following ACF2 commands:

```
SET PROFILE(USER) DIV(OPERPARM)
INSERT userid AUTH(INFO)
```

and compile the following rule sets:

```
$KEY(MVS) TYPE(OPR)
     MCSOPER.userid UID(userid) SERVICE(READ) LOG
$KEY(CONSOLE) TYPE(TSO)
     UID(opermask) SERVICE(READ) LOG
```

The DISA STIG provides the following techniques related to the above recommendations which further expand on the controls and the responsibilities of individuals within the organization. For additional information for each "policy bullet" including the short description identifier and the severity codes refer to the DISA STIG.

- The system programmer will ensure that the CONSOLxx members are properly configured.
- The IAO will ensure that all consoles identified in the CONSOLxx members are defined to the ACP.
- The IAO will ensure that OS/390 Sensitive System Commands are defined to the OPERCMDS resource class. Only a limited number of authorized people are able to issue these commands. All access is logged.

Refer to the DISA O/S 390 & z/OS STIG, V5R2, Volume 1, Section 3.2.5.5 MCS Console Controls, Section 2.1.2.12 MCS Consoles.

3.3.2 CONTROLLING SYSTEM COMMANDS

This document has discussed various system commands, also referred to as operator commands, and the risks and controls associated with them. OS/390 system command controls are provided via resources in the OPERCMDS resource class. This class should already be active and use generic masking. Further system commands can be controlled by the ACP, the sample commands shown below include the relevant ACP commands for the sake of completeness.

The DISA STIG recommends the following in regards to controlling system commands within ACF2; please note that responsibilities delegated to the IAO should be performed by an individual with appropriate knowledge and authority within the organization.

1) Prevent access to the OS/390 resources by default, and log all access. Create generic and specific resource rules with logging as required using the resources defined within the DISA STIG Table A-29, Controls on OS/390 System Commands (volume 1). For example:

```
$KEY(MVS) TYPE(OPR)

UID(-)

ACTIVATE UID(-)

CANCEL.JOB.- UID(-) LOG

CONTROL.- UID(-) SERVICE(READ)

DISPLAY.- UID(-) SERVICE(READ)

MONITOR UID(-) SERVICE(READ)

STOPMN UID(-) SERVICE(READ)
```

2) Only grant access to OS/390 system commands to the extent documented in the installation SOP. Additional profiles are to be defined similarly to those documented above if the existing resource names are too specific or too generic for the controls in the SOP. The rules include the SERVICE (level) and PERMIT/LOG values specified in the SOP or LOG if not specified.

   - The following is an example of granting user userid permission to issue commands against jobs with names beginning pfx, after obtaining permission from the IAO:

     ```
     $KEY(MVS) TYPE(OPR)

     CANCEL.JOB.pfx* UID(userid) SERVICE(UPDATE) LOG

     MODIFY.JOB.pfx* UID(userid) SERVICE(UPDATE) LOG

     STOP.JOB.pfx* UID(userid) SERVICE(UPDATE) LOG
     ```

   - The following is an example of granting to operators whose UID string matches opergrp permission to issue ROUTE commands to sysid during PRIME shift, after obtaining permission from the IAO:

     ```
     $KEY(MVS) TYPE(OPR)
     ```

```
ROUTE.CMD.sysid UID(opergrp) SERVICE(READ) LOG
SHIFT(PRIME)
```

The DISA STIG provides the following technique related to the above recommendations which further expand on the controls and the responsibilities of individuals within the organization. For additional information for each “policy bullet” including the short description identifier and the severity codes refer to the DISA STIG.

- The IAO will ensure that OPERCMDS resource class is active.

Refer to the DISA O/S 390 & z/OS STIG, V5R2, Volume 1, Section 3.2.5.6 OS/390 System Command Controls.

3.3.3 CICS TRANSACTION CONTROL

Customer Information Control System (CICS) is a system utility that allows an authorized user the ability to connect from their terminal to run transactions and application processing on the mainframe. CICS invokes application programs in response to transactions entered at terminals.

Every CICS region can be secured using the ACF2/CICS sub-product. ACF2 uses information within a logonid record to determine access by CICS. It is recommended to the organization require individual CICS users to sign on to the CICS region. This will ensure accountability and appropriate access control. CICS sign-on is optional with the ACF2 CICS interface. Therefore if a terminal runs under CICS but a sign-on has not been performed ACF2 will use the organizations defined default logonid for validating terminal requests.

The DISA STIG, volume 2, discusses controls for CICS transaction control within ACF2. The following sections should be reviewed. In addition, the organization should ensure that controls are in place for any utility that allows connections to the mainframe, such as TSO.

ACF2/CICS Security Related System Initialization Parameters

CICS Region Logonid Controls

CICS User Control

CICS Transaction Control

Refer to the DISA O/S 390 & z/OS STIG, V5R2, Volume 2.

4 CONCLUSION

This document is meant to relay pertinent information within the STIG to CMS and applicable CMS Contractors. This document does not cover all topics discussed in the DISA STIG and is not intended to be used as a substitute to the STIG. In addition, access privileges denoted within this document and DISA STIG may not be suitable for every organization, meaning that each organization may choose to be more restrictive. Because every organization is unique not all aspects of this document or the DISA STIG may be applicable.

This document is to be used as a guide to securing organization environments, and by following the recommendations and techniques within organizations will be able to secure the confidentiality and integrity of their data and resources.

Appendix A – CMS Minimum Security Requirements (CMSRs)

Refer to *CMS Information Security Acceptable Risk Safeguards (ARS) Including CMS Minimum Security Requirements*, Appendix A, *CMS Minimum Security Requirements for High Impact Level Data*, for the applicable CMSRs.

Appendix B - Glossary and Acronym Listing

ACEE	Access Control Environment Element
ACF2	Access Control Facility 2
ACID	Accessor ID
ACPs	Access Control Products
APF	Authorized Program Facility
BLP	Bypass Label Processing
CA	Computer Associates or Certificate Authority
CAISSF	CA's International Standard Security Facility
CDT	Class Descriptors Table
CICS	Customer Information Control System
CMP	Change Management Process
CMS	Centers for Medicare and Medicaid Services
CMSRs	CMS Minimum Security Requirements
CPU	Central Processing Unit
CWF	Common Working File
DAA	Designated Approval Authority
DAT	Dynamic Access Translation
DCA	Departmental Control Acid
DD	Data Definition
DHCP	Dynamic Host Configuration Protocol
DISA	Defense Information System Agency
DMERCs	Durable Medical Equipment Regional Carriers
DoD	Department of Defense
EDC	Enterprise Data Centers
ETMS	External Tape Management System
FI	Fiscal Intermediary
FTP	File Transfer Protocol
FTPD	File Transfer Protocol daemon program

FTPDNS	File Transfer Protocol server program
GSO	Global Systems Options
HFS	Hierarchical File System
HHS	Health and Human Services
HLQ	High Level Qualifier
IAC	Installation Account Code
IANA	Internet Assigned Numbers Authority
IAO	Information Assurance Officer
IBM	International Business Machines
ICS	Internet Connection Sharing
IMS	Information Management System
IP	Internet Protocol
IPL	Initial Program Load
ISPF	Interactive System Productivity Facility
IT	Information Technology
I/O	Input/Output
JCL	Job Control Language
JWT	Job Wait Time
LAN	Local Area Network
LID	Logonid
LSCA	Limit Control ACID
LU	Logical Unit
MAC	Medicare Administrative Contractors
MCS	Multiple Console Support
MSCA	Master Security Control ACID
MUSASS	Multi User Single Address Space System
MVS	Multi-Processing Virtual Storage or Multiple Virtual Systems
NCP	Network Control Program
OIG	Office of the Inspector General
O/S	Operating System

PADS	Program Access to Data Sets
PPGM	Protected Program List
PPT	Program Properties Tables
PROC	JCL procedure
RACF	Resource Access Control Facility
SAF	System Authorization Facility
SCA	Security Control ACID
SDLC	Synchronous Data Link Control
SDSF	System Display and Search Facility
SID	SMF System ID
SMF	System Management Facilities
SNA	System Network Architecture
SPECLU	Specified Logical Unit
SSL	Secure Sockets Layer
STC	Started Task Control
STIG	Security Technical Implementation Guide
SVC	Supervisor Calls
TLS	Transport Layer Security
TSO	Time Sharing Option
TSS	TOP SECRET
USS	Unformatted System Services
VCA	Divisional Control ACID
VTAM	Virtual Telecommunication Access Method
ZCA	Zone Control ACID

References

- IBM International Technical Support Information. (May, 1996). *Planning for a CA-ACF2 Migration to OS/390 Security Sever (RACF)* Redbook.
- OS/390-Z/OS Security. (2004). *Audit and Control Features.* Peter Thingsted
- IBM International Technical Support Information. (October, 2002). *Communications Server for z/OS V1R2 TCP/IP Implementation Guide Volume 2: UNIX Applications* Redbook.
- The Henderson Group. (February, 2006). *How to Audit MVS, RACF, ACF2, CICS, and DB2 Security*.
- Computer Associates International, Inc. (2001). *CA-ACF2 Administrators Guide.* Islandia, New York.
- Computer Associates International, Inc. (2001). *CA-ACF2 Auditors Guide.* Islandia, New York.
- IBM. (April 2006). *Introduction to New Mainframe: Networking*. Mike Ebbers, Wayne O'Brien, Bill Ogden.
- IBM (July 2006). *Introduction to New Mainframe: z/OS Basics.* Mike Ebbers, Chris Hastings.
- http://www.sdsusa.com/dictionary/
- http://www-03.ibm.com/systems/z/
- http://publib.boulder.ibm.com/infocenter/zoslnctr/v1r7/index.jsp